Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] 1. A method of communicating information between users of a communication system includes the following steps of:

generating a module V over a ring R;

generating an outer component P of encryption key that includes sequence (p_1, p_2, ..., p_k) where each member p_j of the sequence belongs to the set {1, 2, ... , m} (the length k of the sequence is arbitrary and thus repetitions are allowed in the sequence);

generating an inner component Q of encryption key that includes elements v_1, v_2, ..., v_m of V and automorphisms g_1, g_2, ... , g_m of V;

generating the encryption key K = (P; Q), where P is the outer component and Q is the inner component;

generating an encryption automorphism T_e of V based on the encryption key K, where T_e includes a composition of certain automorphisms T_1, T_2, ... , T_m of the module V, which composition is performed in the order prescribed by P;

generating an encrypted message element E as a function of a message element M in V and of the encryption automorphism T_e;

transmitting the encrypted message element E along with the outer component P from one user to another;
generating the outer component P' of decryption key that includes sequence (p_k, p_{k-1}, ..., p_1), i.e., the sequence that is reversed of that involved in producing the outer component P of the encryption key;
generating the decryption key K' = (P'; Q'), where P' is the outer component of the decryption key and Q' is the inner component of the decryption key which is equal to the inner component Q of the encryption key;
generating a decryption automorphism T_d of V based on the decryption key K', where T_d includes a composition of the automorphisms T_1, T_2, ... , T_m , which composition is performed in the order prescribed by P', e.g., T_d is the inverse automorphism of T_e;
determining the message element M as a function of the encrypted message element E and of the decryption automorphism T_d, where the function is the same as that one used in generation of E (that is, the decryption method is symmetric to encryption: the decryption proceeds as the encryption, but with replacement of the outer component P with the outer component P').

[c2] 2. The method as defined by claim 1, wherein the ring R is any commutative or non-commutative ring.

[c3] 3. The method as defined by claim 1, wherein said V is a projective module over the ring R.

[c4] 4. The method as defined by claim 1, wherein said V is a free R-module of dimension n, and where n is an integer greater than 1.

[c5] 5. The method as defined by claim 4, wherein the R-module V is the standard free module R^n, that is, V is the set of all n-tuples $x = [x_1, x_2, \ldots, x_n]$ of elements of R.

[c6] 6. The method as defined by claim 2, wherein said ring R is the field of real numbers.

[c7] 7. The method as defined by claim 2, wherein said ring R is the skew-field of quaternions.

[c8] 8. The method as defined by claim 2, wherein said ring R is a finite field.

[c9] 9. The method as defined by claim 2, wherein the ring R is the ring of matrices over the field of real numbers.

[c10] 10. The method as defined by claim 1, wherein said step of generating said automorphisms $T_1, T_2, \ldots, T_m$ further comprises generating automorphisms $T_1, T_2, \ldots, T_m$ of finite orders.

[c11] 11. The method as defined by claim 10 further com-

prises generation of each automorphism T_i of the order 2.

[c12] 12. The method as defined by claim 10, wherein said index i is used in the derivation of said outer component of the encryption or decryption keys and said element T_i is a part of said encryption and decryption automorphisms.

[c13] 13. The method as defined by claim 1, wherein said message element M is an element of said module V.

[c14] 14. The method as defined by claim 13, wherein the encrypted message element E is obtained by applying said automorphism T_e (as defined in the claim 1) to the message element M.

[c15] 15. The method as defined by claim 1, wherein said encrypted message element is produced by a user at one location, transmitted from said one location to another location, and decrypted by a user at said another location.

[c16] 16. A method of communicating information between users of a communication system, the method comprising the steps of:
generating a module V over a ring R; generating an outer component P of encryption key: $P = (p_1, p_2, \ldots, p_k)$

where each member p_j of the sequence belongs to the set {1, 2, ... , m};

generating an inner component Q of encryption key that includes elements $v_1, v_2, \ldots v_m$ of said module V and automorphisms $g_1, g_2, \ldots, g_m$ of V;

generating the encryption key K = (P; Q), where P is the outer component and Q is the inner component;

generating an encryption automorphism T_e of the module V based on automorphisms $T_1, T_2, \ldots, T_m$ of the module V and on the outer component $P = (p_1, p_2, \ldots, p_k)$ of encryption key: $T_e = T_{p1} \circ T_{p2} \circ \ldots \circ T_{pk}$. That is, T_e is an automorphism of the module V obtained as a composition of automorphisms $T_1, T_2, \ldots, T_m$, which composition is performed in the order prescribed by P;

generating an encrypted message element E as a function of a message element M in V and of the encryption automorphism T_e;

transmitting the encrypted message element E along with the outer component P from one user to another;

generating an outer component $P'=(p_k, p_{k-1}, \ldots, p_1)$, i.e., the sequence that is reversed of that involved in producing the outer component P of the encryption key;

generating the decryption key K' = (P'; Q'), where P' is the outer component of the decryption key and Q' is the inner component of the decryption key which is equal to the inner component Q of the encryption key;

generating a decryption automorphism T_d of the module V based on automorphisms T_1, T_2, ..., T_m of the module V and on the outer component $P' = (p_k, p_{k-1}, ..., p_1)$ of the decryption key: $T_e = T_{pk} \circ ... \circ T_{p2} \circ T_{p1}$, where T_1, T_2, ... , T_m are the same automorphisms of V which have been used in the construction of the encryption automorphism T_e;

determining the message element M as a function of the encrypted message element E and of the decryption automorphism T_d, where the function is the same as that one used in generation of E (that is, the decryption method is symmetric to encryption: the decryption proceeds as the encryption, but with replacement of the outer component P with the outer component P').

[c17] 17. The method as defined by claim 16, wherein said encrypted message element M is produced as

$E = T_e(M)$,

where $T_e(M)$ is the element of V obtained by applying the automorphism T_e to said message element M.

[c18] 18. The method as defined by claim 16, wherein said decrypted message element M is produced as

$M = T_d(E)$,

where $T_d(E)$ is the element of V obtained by applying the automorphismT_d to said encrypted message element E.

[c19] 19. The method as defined by claim 16, of further selecting non-zero elements $v_1, v_2, \ldots, v_m$ of the module V.

[c20] 20. The method as defined by claim 16, of construction of R-linear maps $l_p: V \to R$, for p = 1, 2, ..., m, such that $l_p(v_p) = 2$.

[c21] 21. The method as defined by claim 16, wherein said step of generating said automorphisms $T_1, T_2, \ldots, T_m$ of V includes selecting automorphisms $g_1, g_2, \ldots, g_m$ of V and reflections $S_1, S_2, \ldots, S_m$ of V.

[c22] 22. The method as defined by claim 21, wherein said elements $T_1, T_2, \ldots, T_m$ are defined by:
$T_p = g_p \circ S_p \circ h_p$,
where h_p is the inverse automorphism of g_p, that is,
$g_p \circ h_p = h_p \circ g_p$ = the identity automorphism of V,
and S_p is the reflection of V relative to the element v_p, as defined in claim 19, and an R-linear map $l_p: V \to R$ as defined in claim 20. That is, S_p is defined by:
$S_p(x) = x - l_p(x) \cdot v_p$
for any x in V.

[c23] 23. The method as defined by claim 21 where each g_i is a polynomial automorphism of the module V. By definition, a map g: U→V from a R-module U to R-module V is called polynomial map if for any elements $u_1, u_2, \ldots, u_r$

of U there is a finite family of elements v_J labeled by finite sequences $J = (j_1, j_2, \ldots)$ of indices each of which belongs to the set $\{1, 2, \ldots, r\}$ such that for any elements $a_1, a_2, \ldots, a_r$ of R one has:

$g(a_1 \cdot u_1 + a_2 \cdot u_2 + \ldots + a_r \cdot u_r) = \Sigma({}^{a}j_1 \cdot {}^{a}j_2 \cdots {}^{a}j_r) \cdot v_J$,

where summation is over all $J = (j_1, j_2, \ldots)$ as above. A map $g: V \to V$ is a polynomial automorphism if g is invertible and both g and inverse of g are polynomial maps.

[c24] 24. The method as defined by claim 21 where each g_i is a rational automorphism of the module V. By definition, a partially defined map $g: U \to V$ from a R-module U to R-module V is called rational if there exists a polynomial map $f: U \to R$ and a polynomial map $h: U \to V$ such that $h(u) = f(u) \cdot g(u)$ for all u in the domain of g.

[c25] 25. The method as defined by claims 5 and 23 of constructing polynomial automorphisms g_i of the free module $V = R^n$, where each g_i belongs to that group of polynomial automorphisms of V which is generated by all R-linear invertible maps $V \to V$ and by all the polynomial automorphisms $g: V \to V$ of the form:

$g(x_1, x_2, \ldots, x_n) = (x_1, x_2 + f_1(x_1), x_3 + f_2(x_1, x_2), \ldots, x_n + f_{n-1}(x_1, x_2, \ldots, x_{n-1}))$,

where $f_i : R^i \to R$ for $i = 1, 2, \ldots, n-1$ are polynomial maps.

[c26] 26. The method as defined by claims 5 and 24 of constructing rational automorphisms g_i of the free module $V = R^n$, where each g_i belongs to that group of rational automorphisms of V which is generated by all R-linear invertible maps $V \to V$ and by all the rational automorphisms $g: V \to V$ of the form:

$g(x_1, x_2, \dots, x_n) = (x_1, x_2 + f_1(x_1), x_3 + f_2(x_1, x_2), \dots, x_n + f_{n-1}(x_1, x_2, \dots, x_{n-1}))$,

where $f_i : R^i \to R$ for $i = 1, 2, \dots, n-1$ are rational maps.

[c27] 27. The method for construction of rational automorphisms $f_i : R^i \to R$, as of claim 26, where the domain of each f_i is the entire R^i, where R is the field of real numbers as in claim 6.

[c28] 28. The method of claim 27, where each f_i is of the form:

$f_i(x_1, x_2, \dots, x_i) = P_i(x_1, x_2, \dots, x_i)/Q_i(x_1, x_2, \dots, x_i)$,

where $P_i(x_1, x_2, \dots, x_i)$ and $Q_i(x_1, x_2, \dots, x_i)$ are polynomials with real coefficients in the variables $x_1, x_2, \dots, x_i$ such that $Q_i(x_1, x_2, \dots, x_n) > 0$ for any real numbers $x_1, x_2, \dots, x_n$.

[c29] 29. The method as defined by claim 22, of further construction of the R-linear map $l_p : V \to R$ by means of a map $L: V \times V \to R$, which is left R-linear, that is,

$L(a \cdot x + b \cdot y, v) = a \cdot L(x,v) + b \cdot L(y,v)$

for any elements x, y, and v of V, and any elements a and b of R, where '·' stands for the action of the ring R on the module V.

[c30] 30. The method of selecting elements $v_1, v_2, \ldots, v_m$ of the claim 19 that provides that $L(v_p, v_p) \neq 0$ for each p= 1, 2, ..., m.

[c31] 31. The method as defined by claim 29, of further selecting elements $v_1, v_2, \ldots, v_m$ satisfying the property that for each p= 1, 2, ..., m there exists an element r_p in R such that $L(v_p, v_p)\cdot r_p = 2$.

[c32] 32. The method of claims 20, 29, and 31 for construction of a R-linear map $l_p : V \to R$ by

$l_p(x) = L(x,v_p)\cdot r_p$

for all x in V, p = 1, 2, ..., m.

[c33] 33. The method of claims 6, 20, 30, and 32 for construction of a R-linear map $l_p : V \to R$ by

$l_p(x) = 2L(x,v_p)/L(v_p,v_p)$

for all x in V, p = 1, 2, ..., m.

[c34] 34. The method of claims 6, 20, 22, 30, and 32 for construction of a reflection $S_p : V \to V$ by

$S_p(x) = x - 2L(x,v_p)/L(v_p,v_p)\cdot v_p$

for all x in V, p = 1, 2, ..., m.

[c35] 35. The method as defined by claims 5 and 29, wherein the left R-linear map L is a bi-linear form on $V = R^n$, i.e., $L(x,y) = x_1 \cdot f_1(y_1) + x_2 \cdot f_2(y_2) + \ldots + x_n \cdot f_n(y_n)$, where each $f_i : R \rightarrow R$ for i = 1, 2, ..., n is a polynomial.

[c36] 36. The method as defined by claims 5 and 29, wherein the left R-linear map L on $V = R^n$ is further defined by: $L(x,y) = \Sigma x_i \cdot l_{i,j} \cdot y_j$ for any x, y $\in R^n$, where the summation is over all pairs (i,j) such that $1 \leq i,j \leq n$, and $l_{i,j}$ in R for i = 1, 2, ..., n and j = 1, 2, ..., n.

[c37] 37. The method as defined by claim 36, wherein the left R-linear map L is the standard bilinear form on $V = R^n$ further defined by: $L(x,y) = x_1 \cdot y_1 + x_2 \cdot y_2 + \ldots + x_n \cdot y_n$.

[c38] 38. The method as defined by claim 36, wherein the left R-linear map L is defined by: $L(x,y) = x_1 \cdot (y_1)^3 + x_2 \cdot (y_2)^3 + \ldots + x_n \cdot (y_n)^3$.

[c39] 39. The method as defined by claim 16, wherein said encrypted message element E is produced by a user at one location, transmitted from said one location to another location, and decrypted by a user at said another location.

[c40] 40. The method as defined by claim 6, wherein each said

real number is represented as decimal number with a prescribed number of decimal places after the dot.

[c41] 41. The method as defined by claim 40, wherein each said number is an integer.

[c42] 42. A method of communicating information between users of a communication system, the method comprising the steps of:

means for generating a module V over a ring R;

means for generating an outer component P of encryption key that includes sequence $(p_1, p_2, \ldots, p_k)$ where each member p_j of the sequence belongs to the set {1, 2, ..., *m*};

means for generating an inner component Q of encryption key that includes elements $v_1, v_2, \ldots, v_m$ of V and automorphisms $g_1, g_2, \ldots, g_m$ of V;

means for generating the encryption key K = (P; Q), where P is the outer component and Q is the inner component; means for generating an encryption automorphism T_e of V based on the encryption key K, where T_e includes a composition of certain automorphisms $T_1, T_2, \ldots, T_m$ of the module V which composition is performed in the order prescribed by P;

means for generating an encrypted message element E as a function of a message element M in V and of the encryption automorphism T_e;

means for transmitting the encrypted message element E along with the outer component P from one user to another;

means for generating the outer component P' of the decryption key that includes sequence (p_k, p_{k-1}, ..., p_1), i.e., the sequence that is reversed of that involved in producing the outer component P of the encryption key;

means for generating the decryption key K' = (P'; Q'), where P' is the outer component of the decryption key and Q' is the inner component of the decryption key which is equal to the inner component Q of the encryption key;

means for generating a decryption automorphism T_d of V based on the decryption key K', where T_d includes a composition of the automorphisms T_1, T_2, ..., T_m , which composition is performed in the order prescribed by P', e.g., T_d is the inverse automorphism of T_e;

means for determining the message element M as a function of the encrypted message element E and of the decryption automorphism T_d, where the function is the same as that one used in generation of E (that is, the decryption method is symmetric to encryption: the decryption proceeds as the encryption, but with replacement of the outer component P with the outer component P').

[c43] 43. The system as defined by claim 42, wherein said en-

crypted message element is produced by a user at one location, transmitted from said one location to another location, and decrypted by a user at said another location.